John R. Christiansen, J.D.
Christiansen IT Law
Privacy/Security/Compliance

2212 Queen Anne Avenue North #333
Seattle, Washington 98109
206.301.9412
christiansenlaw@comcast.net

Jeff Hummel, MD, MPH
Medical Director for Clinical Informatics, Qualis Health

Connecting for Health Common Framework

Presentation to the Washington State Health Information Infrastructure Advisory Board

April 27, 2006

Connecting for Health

- More than 100 leading private and public organizations participate in Connecting for Health, including experts in clinical medicine, information technology, public policy, consumer concerns, and patient privacy. . . . Connecting for Health was created by the Markle Foundation, and, is led and managed by Markle. The collaborative is funded by both Markle and the Robert Wood Johnson Foundation.

Connecting for Health

- Markle Foundation

  Mission: “Emerging information and communication technologies possess enormous potential to improve people's lives. The Markle Foundation works to realize this potential by accelerating the use of these technologies to address critical public needs, particularly in the areas of health and national security.”

Connecting for Health

- “Blue Ribbon” Steering Group
  - Healthcare associations, major technology companies/healthcare technology vendors, thought leaders, etc.
- “HHS Awards Contracts to Develop Nationwide Health Information Network”
  - “CSC, working with Browsersoft, Business Networks International, Center for Information Technology Leadership, Connecting for Health, DB Consulting Group, eHealth Initiative, Electronic Health Record Vendors Association, Microsoft, Regenstrief Institute, SiloSmashers, and Sun Microsystems. This group will work with the following health market areas: Indiana Health Information Exchange (Indiana); MA-SHARE (Massachusetts); and Mendocino HRE (California)”

Common Framework

- Underlying concept: “Information exchange can take place among existing and future health care networks if all participants adhere to a small set of shared rules – a ‘Common Framework’ of technical and policy guidelines.”
- “Common, non-proprietary technical and policy standards that can work with information systems already in place.”
- “All of the . . . Common Framework resources are available . . . at no cost.”

Nine Principles

- Openness and transparency
- Purpose specification and minimization
- Collection limitation
- Use limitation
- Individual participation and control
- Data integrity and control
- Security safeguards and controls
- Accountability and oversight
- Remedies

Basic Terminology

- Subnetwork Organization (SNO) – Legal and technical implications
- Inter-SNO Bridge (ISB) – How SNOs connect
- Record Locator Service (RLS) – How SNOs allow participants to share patient records

SNO: Legal Implications

- “An affiliation of users who share health information and adhere to a common IT framework. Like RHIOs, subnetworks can be regionally or geographically based, and some cross state or other jurisdictional boundaries.”
- RHIOs, enterprise networks, research communities, etc.
- Minimum requirement: Governed by contractual agreement to use same RLS
- Inter-SNO traffic is via ISB
    - Bloomrosen & Heubusch, *The Language of Health Data Exchange* (J. AHIMA, April 2006)

Common Framework Model Contract

1. Introduction
2. Definitions
3. SNO Usage Terms and Conditions
4. Registration (Agreement to Participate in SNO)
5. Authorized Users
6. Data Recipient’s Right to User Services
7. Data Provider’s Obligations (to Provide Accurate Data, Limit Data Uses)
8. SNO Software/Hardware License
9. Protected Health Information Compliance (Including Business Associate Provisions)
10. Participant Compliance Obligations (Including Security)
11. SNO Operations and Responsibilities
12. Fees and Charges
13. Proprietary Information
14. Disclaimers, Exclusions, Warranties, Liabilities, Indemnification
15. Insurance
16. General

Common Framework Policies

P1: Privacy Architecture

P2: Model Privacy Policies and Procedures

P3: Notification and Consent When Using a Record Locator Service

P4: Correctly Matching Patients with Their Records

P5: Authentication of System Users

P6: Patients' Access to Their Own Health Information

P7: Auditing Access to and Use of a Health Information Exchange

P8: Breaches of Confidential Information

Common Framework Technical Guides

T1: Technical Issues and Requirements

T2: Health Information Exchange Architecture

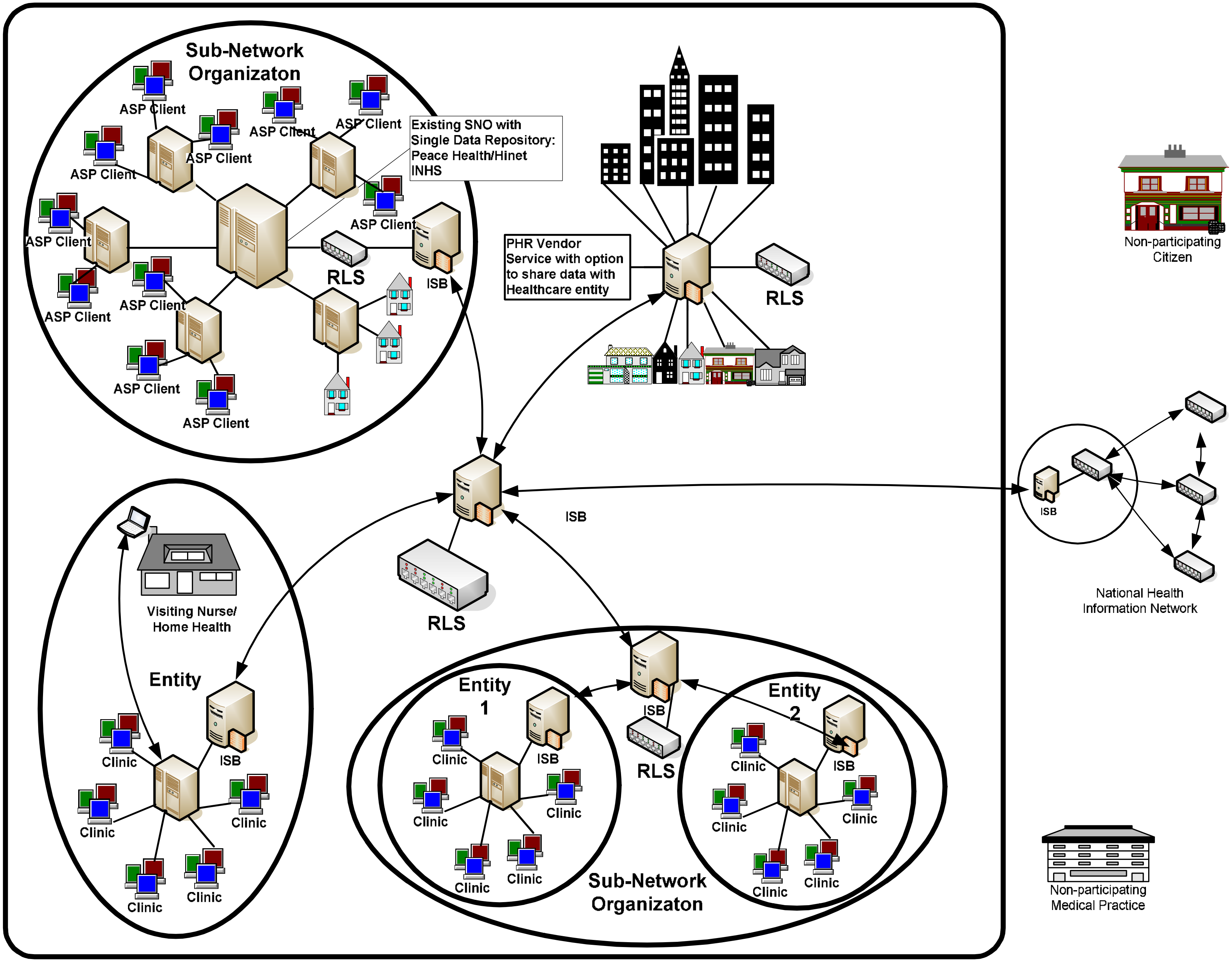
T3: Medication History Standards

T4: Laboratory Results Standards

T5: Background Issues on Data Quality

T6: Record Locator Service Background (From MA Prototype)

Common Framework Architecture



Entity

“A functionally independent participant in the healthcare system”

- Single doctor’s office practice: Marcus Welby, MD
- Staff model HMO: Group Health, Kaiser
- Multi-specialty group: Everett Clinic
- Independent practice organization: PSFP
- National organization: VA, Pharmacy chain, Network of cancer centers
- Community Clinic System: PSNHC

Record Locator Service: RLS

- One RLS per SNO
- RLS designed only for patient-centered queries
- Two types of transactions
  - Additions, modifications, deletion of record location
  - Request for information about a particular patient
- All transactions logged and audited
- Supports only encrypted web communication
- Designed for authorized demographic info query
- Must support HL7 2.4, may support HL7 3.0
- Support synchronous and asynchronous query

Record Locator Service: RLS (cont)

- Probabilistic matching algorithm
- Return matching demographic records & locator
- Return only records meeting minimum prob level
- No “BTG” to get records below minimum prob level
- RLS will not return demographic data not in query
- SNO must separate demographic and clinical data
- Served data may be cached by providing institution
- RLS must report obvious errors in data received
- Must provider audit log for all published data

Inter-SNO Bridge: ISB

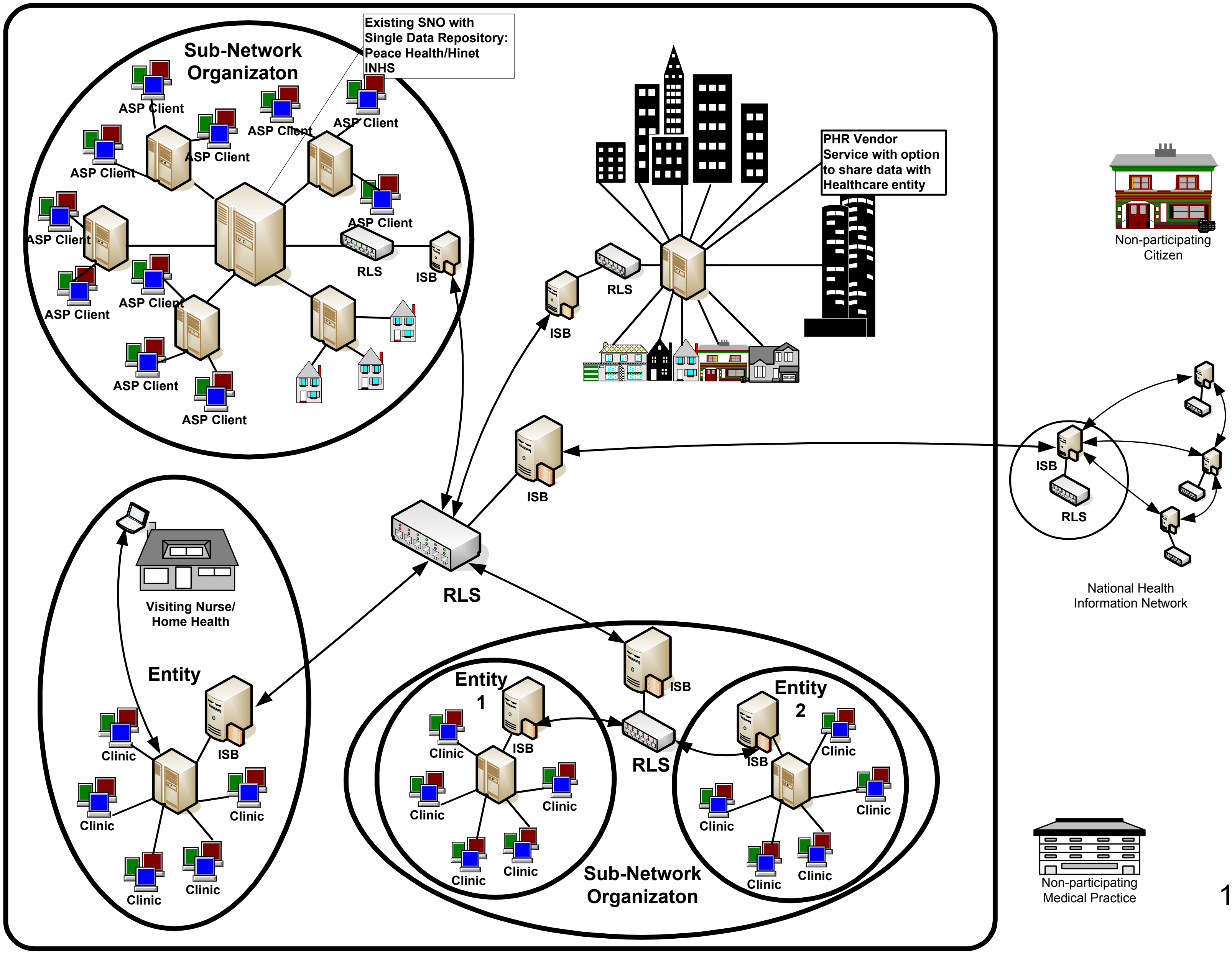
Point of contact between SNOs

- Request for clinical data goes out via ISB
- Interface to data held by SNO used by institutions outside the SNO

Features of ISBs

- 1 ISB per SNO; handles all per pt clinical requests
- ISB is only for patient-centered queries
- All transactions through ISB are logged & audited
- Supports only encrypted web communication
- Must support HL7 2.4, may support HL7 3.0
- Must support two patterns of request
  - 1 pass: Requestor presents pt details; receives records
  - 2 pass: Requestor presents pt details; receives locators; responds with records they would like to access.
- Must support asynchronous record request

Common Framework Architecture



Existing SNO with Single Data Repository: Peace Health/Hinet INHS

PHR Vendor Service with option to share data with Healthcare entity

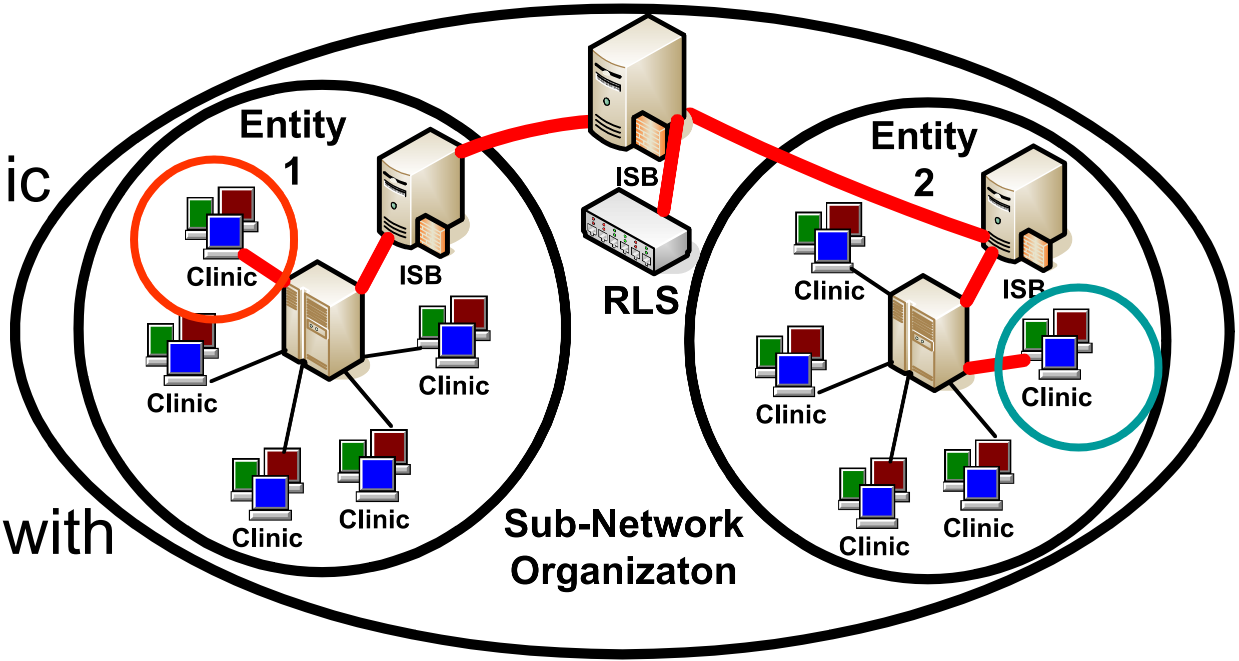
Implementation of Common Framework Architecture

Transfer of Clinical Data Between Entities in a Single SNO

- Asking for record locations
- Aggregating the identified records
- Displaying or otherwise using the records

Step 1: Asking for Record Location

1. Pt presents for first time at clinic with serious symptom
2. Patient provides basic demographic data
3. Clinic queries local RLS
4. Record locations with sufficiently high probability of match are returned from RLS



Step 2: Aggregating the Identified Records

- Client Aggregation:
  - Advantages: refined control over record requests and possibly higher integration with other local electronic data systems.
  - Disadvantages: Higher technical requirements by participating entities in SNO
- Central Aggregation Service:
  - Advantages: creates economies of scale for the SNO
  - Disadvantages: Less control over record by requesting entity and greater security risk

Step 3: Displaying or otherwise using the records

No constraints on how the records are used

- Display records directly to clinician
- Integrating records into the client EMR
- Feeding into decision support tools.

Questions?